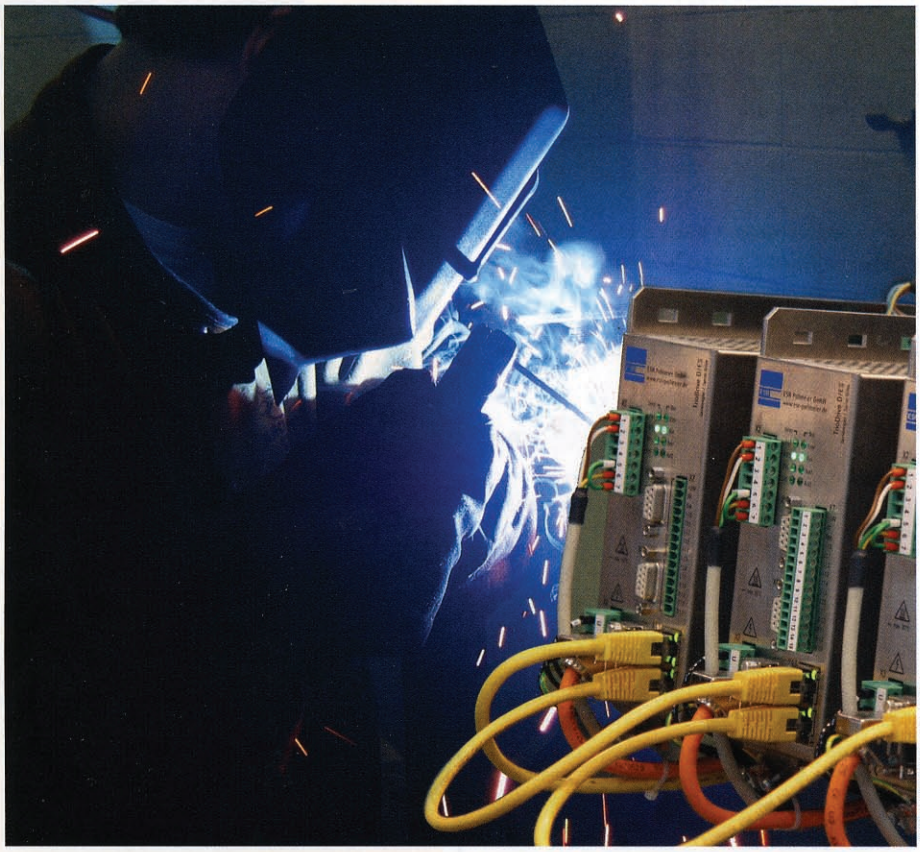
Troubleshooting IE networks requires a special approach...

Ethernet-TCP/IP can look back on an unprecedented 20-year success story. Having conquered telecomms, office and home it continued its march into factory automation. Not only did the components have to adapt to the physical conditions of the manufacturing environment but also to the topologies and deterministic requirements found there. Even trouble-shooting networks based on Industrial Ethernet required a different approach, described here by Inat's Albrecht Petzoldt



ARTWORK: FRANK OGDEN

WHAT DIFFERENTIATES 'Ethernet' from 'Industrial Ethernet'? One could say that the differences are small but crucial. It already begins with the operating environment of the components being used which must satisfy the special requirements of manufacturing plants.

Ensuring an acceptable lifespan for the installed devices needed regard to such operating parameters as temperature (for the steel industry...) dust (in mining...) salt (for marine operation) and so on. Such things have created a major shift in the failure modes encountered with Ethernet used beyond the office world.

For instance, the cables and plug connectors have to be designed for the rugged environments outside the office installation. Protected against dust and temporary immersion in water up to 1m (IP67), the 4-pole M12 plug connector is frequently used. One can say that the RJ45 plug connector has prevailed in office networks, but the diversity of plug connectors for industrial networks is considerably greater and depends primarily on the ambient conditions.

The same applies to the use of network cables. The length of the transmission path determines the transmission medium – whether copper twisted pair or fibre optic cable. Particularly in industrial networks, use of polymer optic fibre (POF) is increasing everywhere where EMC (Electro-Magnetic Compatibility) problems are to be expected (e.g., presence of manufacturing cells with welding robots). The transmission distance tends to be restricted to less than 100m – the typical length for transmission with TP.

The active network components (switches, routers, etc) of Industrial Ethernet are not only adapted to the harsher conditions of factory and process plant but are also designed for DIN rail installation and can be operated with supply voltages (e.g., 24V DC) not generally found in the office world. Otherwise they are almost identical to the components of a conventional Ethernet TCP/IP network.

The protocol decides the approach

The chart (Fig. 1) describes the situation for protocol processing with Industrial Ethernet. The H1 protocol enjoyed wide use with the Siemens Simatic S5. Based directly on Ethernet, it uses only MAC addresses for addressing. This brings with it the disadvantage that the MAC addresses are often configured (or 'parameterised' as automation people would spout jargon) in a way more normally associated with IP addresses. The disadvantage of this protocol is that it has no routing capability and can therefore only be used in a subnetwork. It also follows that remote access as is used for remote maintenance jobs becomes impossible.

The successor to the H1 (ISO) protocol which includes a routing capability is the RFC1006 protocol – also known as 'ISO-on-TCP' in Siemens terminology. It uses services such as data security and data flow control of the TCP/IP protocol for example. But since TCP is stream-oriented, the RFC1006 handles the block recognition required for communication between the controllers. Port 102 is the standard port.

Data blocking is also implemented in the Inat-PLC header but does without the configuration of the TSAPs (Transport Service Access Points) and that simplifies connection setup.

Use of Modbus and the Modbus on TCP

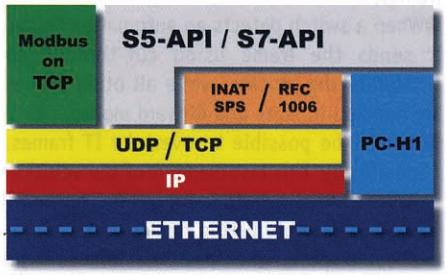


Fig. 1. Protocol processing with Industrial Ethernet determines how you set up or troubleshoot a network. For instance the Siemens H1 protocol bypasses the IP layer altogether – which means that diagnostic tools that require an IP address to function can't be used

protocol is similar to that of the H1 and the RFC protocols. The Modbus protocol was originally developed by Gould-Modicon for communication with its PLCs. The protocol was placed on a physical layer such as RS 232, RS 485 or HDLC. To be able to use it in the Ethernet-TCP/IP world, the successor Modbus on TCP was placed directly on Layer 4 as the name already indicates. Port 502 is the standard port for Modbus on TCP. This protocol is frequently used for communication with devices from companies such as Phoenix, Wago and Beckhoff.

It is interesting to note that, during cabling (Layer 1), automation people frequently ignore Auto-MDI/MDIX interfaces. Auto-Negotiation (AN), taken for granted in office communication, is treated similarly. In the meantime, a fixed setting now predominates so that protocols such as Auto-MDI/MDIX and AN do not spend time negotiating the transmission parameters of any missing ones for the data transmission.

Naturally, interference caused by difficult EMC environments also plays a role since repeated interference activation of these configuration protocols is possible.

In order not to disturb system data communication on the industrial network, the use of active scanners (for viruses, ports, SNMP clients and so on) is also rare. Passive scanners are used if anything for network analysis. These only record existing data communication and extract the necessary information via network stations and their communication connections.

Topology of an industrial network

The architecture of an industrial network has three levels. The process control level represents the conventional company network based on Ethernet and TCP/IP. It contains all the network components of a company network such as file server, application server (e.g., ESP system), data server and Internet accesses.

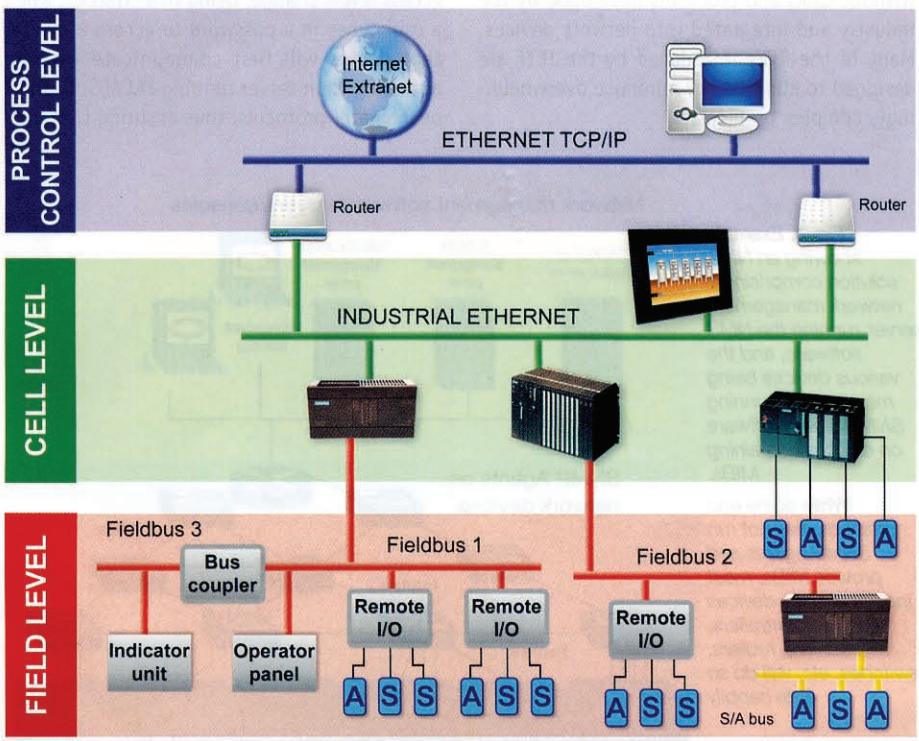
During the past decade, Industrial Ethernet has firmly established itself at the cell level located underneath which represents the communication platform occupied by the system controllers.

The lowest level is the fieldbus level which contains the sensors (for obtaining measuring data) and actuators (for transmitting reference variables to the devices to be controlled). The actuators and sensors are connected to the system controllers directly or via fieldbus systems such as Profibus, Interbus, and so on.

Ethernet has already begun to compete with the field and device level systems at the traditional fieldbus level. However, at this level, there are often real-time requirements which exclude the use of 'normal' IEEE 802.3 Ethernet. This is the development driver for Ethernet with the necessary real-time properties. Unfortunately wider industry has not been able to agree on a uniform standard, and each company or company consortium follows its own approach to creating real-time Ethernet.

More than 20 real-time Ethernet solutions are currently on the market. However, only a few solutions will presumably be able to establish themselves permanently.

Even if some companies do run their office networks and system control networks on a single network, opinion has generally taken hold that these networks should be separated from each other by routers or even firewalls. The goal is to protect the system control network from possible interference since this must run day and night with as little downtime as possible. 24-hour operation and the high degree of availability present a great challenge to the operators of these industrial networks. Redundancy concepts for fail-safe operation are in demand.



Diagnostics in case of failure

The capabilities which are built in to the network components provide initial help with trouble-shooting. The Link-LED on the network card and on the Switch indicate a correct connection on Layer 1. The ping or tracert commands at the command level show that a connection to Layer 3 is functioning.

If these tests do not help, diagnostic devices are required. So-called cable verifiers, which test all cable characteristics of a TP cable as per CAT 5e, CAT 6, and CAT 7 in just a few seconds, check the cable infrastructure. Since these devices (Fluke, Agilent, Ideal Industries, ...) are not exactly cheap, service providers can be hired to handle cable certification.

The 'Lanmeters' which were very common just a few years ago are being used less and less. This is not least because the network cards and network components have become astonishingly reliable despite price deterioration.

In the past, faults were primarily looked for in Layers 1 and 2 while today it is mainly the faults in Layers 3 to 7. The most common diagnostic devices for this work are network analysers or Sniffers. These tools are essentially software programs which, together with the network card of a PC or Notebook, constitute a measuring device. Wireshark (formerly Ethereal) software – freeware – is in very wide use. However it was always intended for troubleshooting office automation.

Our own company has developed a purposed designed tool, NetSpector, specifically for Industrial Ethernet networks. Using graphic presentations and easy-to-use filter options, this software simplifies handling of fault conditions considerably. This network analyser consists of two parts – the Recorder for acquiring data and the Viewer for presenting the data. Recorders are installed as listening posts at strategic points in a network. The Viewer can be used – from another location – for flexible connection to these listening posts and for monitoring the data streams.

Designed for purpose

Network analysis requires a knowledge of protocols and a feel for networks. The amount of information that the analyser device can present is enormous. A good Sniffer, several of which are on the market, can make troubleshooting easier.

Albrecht Petzoldt is Head of Training with INAT GmbH, Nürnberg, Germany

FOR MORE INFORMATION CIRCLE **41**